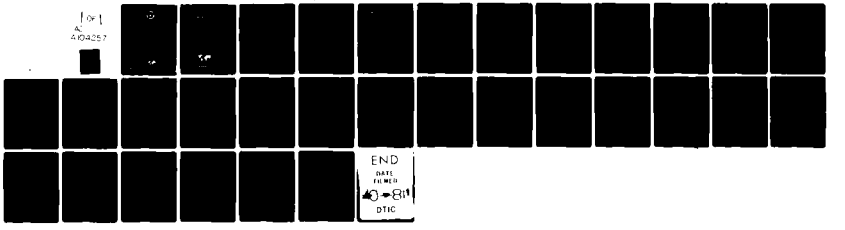
AD-A104 257 HONEYWELL INFORMATION SYSTEMS INC MCLEAN VA F/G 9/2
SECURE SUBSYSTEM RESTRICTIONS.(U)
OCT 80 DCA100-79-C-0011
UNCLASSIFIED NL



LEVEL

AD A104257

Defense Communications Agency

Command and Control Technical Center

Contract DCA 100-79-C-0011

DTIC FILE COPY

DTIC
ELECTE
SEP 16 1981
A

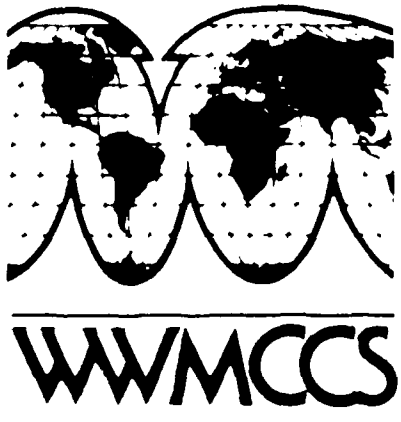
WWMCCS

81 9 03 09

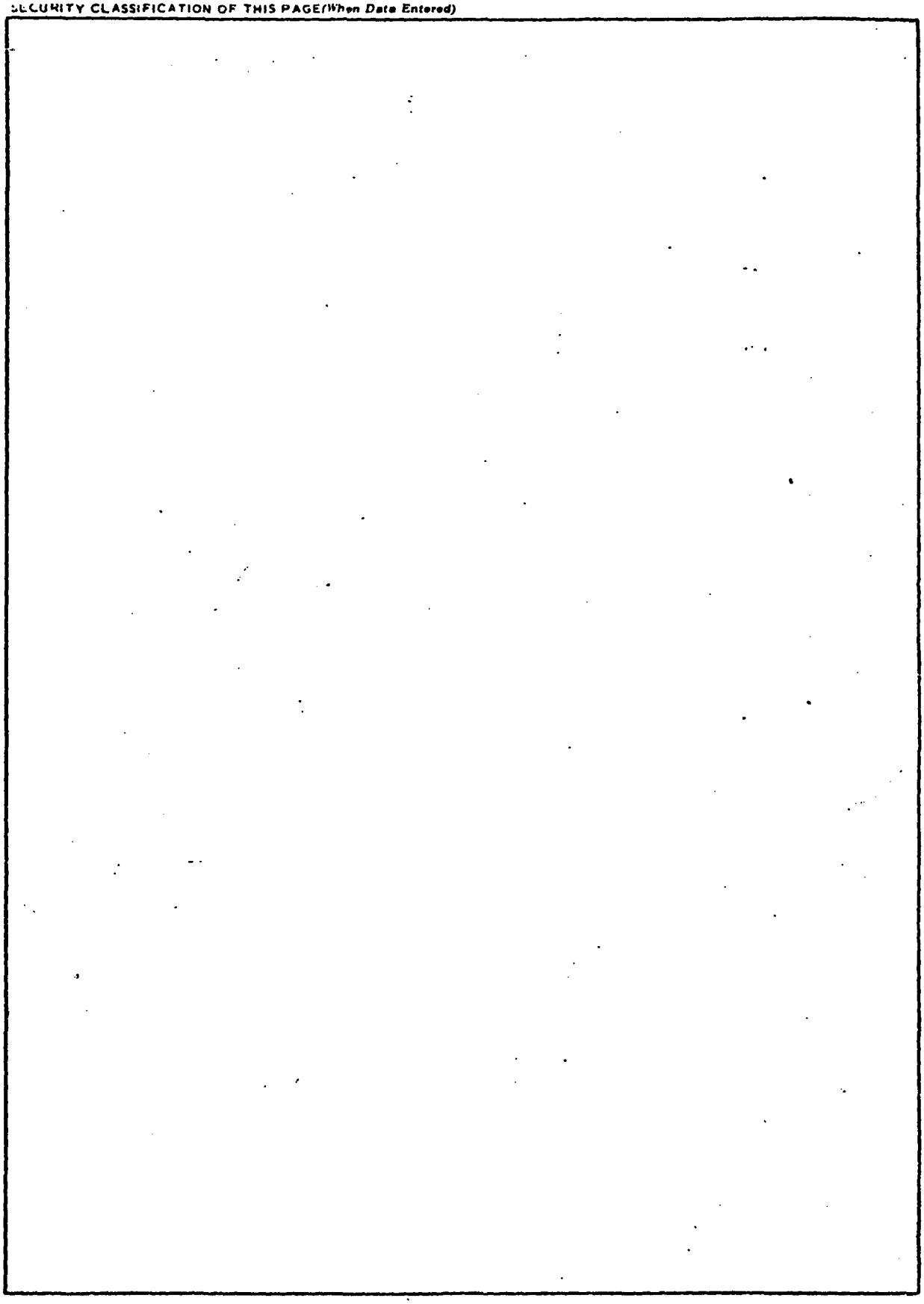
Honeywell

SECURE SUBSYSTEM RESTRICTIONS
TASK 8004

OCTOBER 3, 1980



This document has been approved for public release and sale; its distribution is unlimited.



SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER	2. GOVT ACCESSION NO. / 3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) SECURE SUBSYSTEM RESTRICTIONS	5. TYPE OF REPORT & PERIOD COVERED FINAL REPORT Oct. 3, 1980
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s)	8. CONTRACT OR GRANT NUMBER(s) DCA 100 - 79 - C - 0011 ✓
9. PERFORMING ORGANIZATION NAME AND ADDRESS Honeywell Information Systems, Inc. MCLEAN, VA	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS TASK 8004
11. CONTROLLING OFFICE NAME AND ADDRESS DCA/ C430 11440 ISAAC NEWTON SQ. N RESTON, VA 22090	12. REPORT DATE Oct 3, 1980 / 13. NUMBER OF PAGES
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report) UNCL / 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

UNLIMITED

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Time Sharing System (TSS), RESTRICTIONS, SACLANT

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This document includes a technical report on the changes to TSS and on the structure and security of the Management Data Query System (MDQS). All restricted users are prevented from penetrating outside the MDQS subsystem. A report of all attempts is made.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Honeywell CCTC TASKING STATEMENT 8004

SUBJECT: SECURE SUBSYSTEM RESTRICTIONS

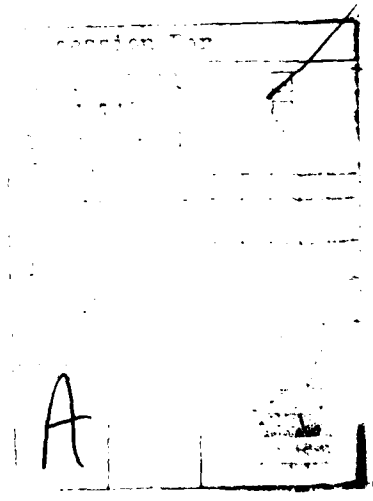
PREPARED FOR: DEFENSE COMMUNICATIONS AGENCY
COMMAND AND CONTROL TECHNICAL CENTER

CONTRACT NUMBER: DCA100-79-C-0011

CONTRACTOR: HONEYWELL INFORMATION SYSTEMS, INC.

PREPARED BY: OPERATING SYSTEMS DEVELOPMENT

DATE: OCTOBER 3, 1980



SECURE SUBSYSTEM RESTRICTIONS
TABLE OF CONTENTS

TABLE OF CONTENTS (CONT)

LIST OF FIGURES

SECTION 1. GENERAL

1.1 Purpose. The objective of this task is to modify the Time Sharing System (TSS) available in the H6000, in order to prevent the restricted user from penetrating outside the MDQS subsystem, and to report any attempts made by the restricted user to do so. Additional constraints will be provided by the following two conditions:

a. The User Profile Systems (UPS's of MDQS) will be used to prevent the use of the PERF and PRIV commands by the restricted user,

b. The restricted USERID will be created in a File Management Supervisor (FMS) activity with no CARDIN, TALK, LODS, or LODX permissions.

The changes to TSS will be implemented so as to allow for the restriction to be a site option.

This document includes a technical report on the changes to TSS and on the structure and security of the Management Data Query System (MDQS). Also included is a report on the characteristics of a user-defined subsystem on the Command Library (CMDLIB) which are necessary to maintain the security of the MDQS environment.

1.2 Project References.

a. CCTC Contractor Tasking Order 8004, SACLANT RNP Software Development, Contract Number DCA100-79-C-0011

b. Honeywell Information Systems, Inc., 7.2B GCOS Listings:

TSSA
TSSH
TSSI
TSSK
SECR

c. Honeywell Information Systems, Inc., 7.2B MDQS Listings

d. Honeywell Information Systems, Inc., MDQS Subroutine Library Listings

e. Honeywell Information Systems, Inc., TSS System Programmer's Reference Manual, DD17D, Rev. 0, 1979

f. CINCLANT Command Library Listings

g. Honeywell Information Systems, Inc., Management Data Query System Administrator's Guide, DD94B, Rev. 2, 1979

h. Honeywell Information Systems, Inc., Management Data Query Systems/IV User's Guide, DD92, Rev. 2, 1978 and Addendum (no date)

i. Joint Technical Support Activity, TCON USER'S GUIDE, January 1975

j. Joint Technical Support Activity, TCON PROGRAMMER/ANALYST GUIDE, January 1975; change 1, June 1978

k. Joint Technical Support Activity, TCON PROGRAM MAINTENANCE MANUAL, January 1975; change 1, June 1978

l. Honeywell Information Systems, Inc., Time Sharing System General Information Manual, DD22, Rev. 0, 1974

m. WWMCCS Supplement Management Data Query System/IV Administrator's Guide (no date)

n. WWMCCS Supplement Management Data Query System/IV User's Guide (no date)

SECTION 2. TSS MODIFICATIONS

2.1 General. This section describes the changes to TSS which are necessary to secure the MDQS environment. Securing the MDQS system will be achieved by inhibiting any TSS function currently available in Software Release 7.2B that would allow the restricted user to:

a. interactively program

b. create and subsequently run any job control language

c. peek and/or modify memory in H6000

d. enter the Time Sharing Master subsystems

Under the proposed TSS modification, an illegal function will be designated by setting bit 18 of the parameters field (currently unused) in the function's program descriptor within TSSA. This bit will then be checked when a restricted user attempts to perform a new function, so that it can be determined if the function is allowed.

2.2 Program Descriptor Format. TSS is designed as an executive or monitor, servicing generic subsystems which consist of two logically and physically separate parts: a program and a program descriptor.

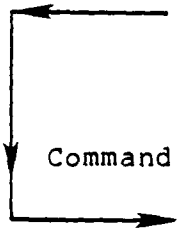
Each TSS function has associated with it a program descriptor which points to a list of primitives. These primitives are interpreted by TSS to control the processes implied when the function is recognized.

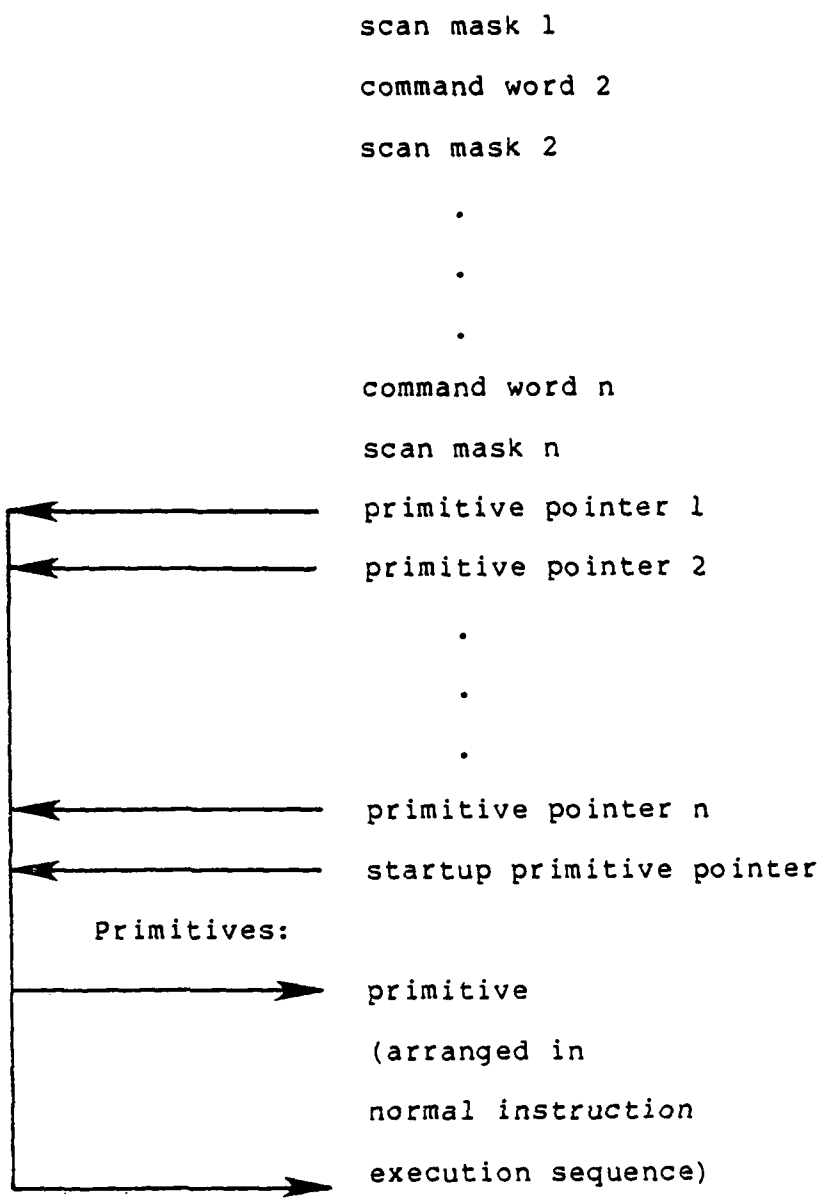
MDQS and CMDLIB Time Sharing programs recognize the TSS command language and initiate process sequences based on these commands.

The functions, descriptors, command language, and primitive lists are contained in the communication region module, TSSA, which consists of three block common areas: .TSCOM, the communication region proper, .TPRGD, the program descriptor block, and .TPCOM, the command language and primitive lists block.

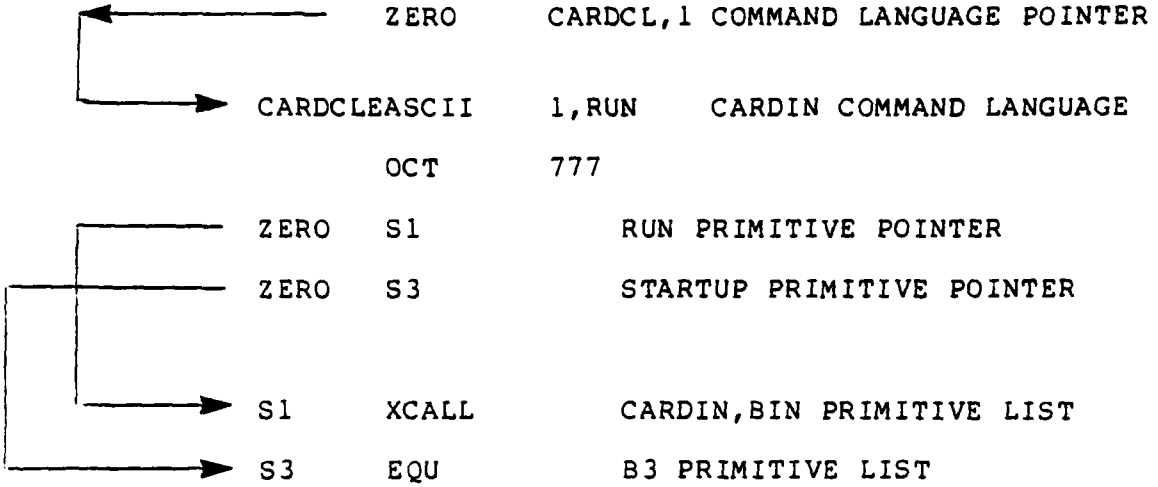
The program descriptor is formatted as follows:

Word	
1	subsystem name in ASCII
2	program size, load size
3	entry point, parameters
Bits	18-24 not defined
	25 DRL SWITCH permitted for SY**
	26 Subsystem cannot be selected at SYSTEM Level
	27 Subsystem allowed use of DRL FILACT, to get a specific function
	28 Execute permission permitted for reads, unless DRL OBJTIM has been executed
	29 Subsystem can query System Master Catalog (SMC)
	30 BASIC or DATABASIC (system selection)
	31 Subsystem uses common command list
	32 Program stored on secondary file #Q
	33 Patches are in patch table
	34 Do not set base register on dispatch
	35 Permitted privileged derails
4	seek address, initial load address
5	command language pointer, number of words in command language




scan mask 1
command word 2
scan mask 2
command word n
scan mask n
primitive pointer 1
primitive pointer 2
primitive pointer n
startup primitive pointer
Primitives:
primitive
(arranged in
normal instruction
execution sequence)

For example, CARD's program descriptor is:



```
CARD    PRGDES   CARD,(CARDCL,1),,.BCMCL
        ASCII    1,CARD
        ZERO
        ZERO     ,.BCMCL
        ZERO     CARDCL,1 COMMAND LANGUAGE POINTER

CARDCLEASCII     1,RUN    CARDIN COMMAND LANGUAGE
        OCT      777
ZERO    S1           RUN PRIMITIVE POINTER
ZERO    S3           STARTUP PRIMITIVE POINTER

S1      XCALL        CARDIN,BIN PRIMITIVE LIST
S3      EQU          B3 PRIMITIVE LIST
B3      STFALS       .SW15,B3.1
B3.1    CALLP        OLDNEW
BIN
```

2.3 Modules Affected.

a. TSSA

b. TSSI

c. TSSH

2.3.1 TSSA. The changes to TSSA involve setting bit 18 of the program descriptor parameter field of all those functions which are to be restricted. The list of restricted functions is included below.

2.3.2 TSSI. The routine to check for a restricted user's attempt to access an illegal function will be incorporated into this module. There are two words within TSSI which must be patched to invoke the restriction. The first word, at symbolic location RESTC1, designates the User Security Matrix (USM) bits that are to be set to 0 for a restricted USERID. The second word, at location RESTC2, specifies the USM bits that are to be set to 1 for a restricted USERID. If, for example, a restricted user is to be designated by bit 20 of the USM to be 0 and bit 22 to be 1, the site option patches would be as follow:

```
1       8       16                  32          73
16310   OCTAL   000000100000        RESTC1      .MTIMS
16311   OCTAL   000000020000        RESTC2      .MTIMS
```

TSSI checks for the bits set in RESTC1 to be 0 in the USM, and then checks for the bits set in RESTC2 to be 1 in the USM. If both these conditions are met, the user is a restricted one. In this case, the program descriptor will be analyzed to determine if the subsystem may be accessed by the restricted user. If not, the security breach code will be set to 76 and a transfer to TSSK will be made to process the breach. If the USM bits corresponding to those set in RESTC1 and RESTC2 are not set to 0 and 1, respectively, then the option has not been selected by the site or the user is not a restricted one. The routine that checks for a restricted user will be entered from TSSI when processing a subsystem startup request.

2.3.3 TSSH. TSSH will be modified to transfer to the TSSI restricted user routine when a CALLP primitive (transfer control to a subsystem) is being processed. This will prevent a restricted user from invoking an illegal function, as well as preventing a legal function from initiating an illegal one.

2.4 Security Recommendations.

2.4.1 Disallowed Functions. The following subsystems may not be utilized by the restricted user:

6.4 Function	7.2B Function	Description
--	ADMN	ADMN Unbundled
ALGO	ALGO	ALGOL Program Language
--	APL	APL Unbundled
--	APLA	APL Unbundled
--	APLB	APL Unbundled
--	APLC	APL Unbundled
--	APLD	APL Unbundled
--	APLE	APL Unbundled
--	APLF	APL Unbundled
--	APLG	APL Unbundled
--	APLH	APL Unbundled
--	APLI	APL Unbundled
--	APLJ	APL Unbundled
--	APLK	APL Unbundled
--	APLL	APL Unbundled
BASI	BASI	BASIC Program Language
BASY	BASY	Run Command For BASIC
BEXP	BEXP	BASIC Executive
--	BRN	COBOL Unbundled
*	CARD	Run Command/Spawns Batch Job
--	COEX	IDS Subsystem Unbundled
CDIN	CDIN	Run Command/Spawns Batch Job
--	CIDS	IDS Subsystem Unbundled
--	CMOD	IDS Subsystem Unbundled
--	COUT	DMS-B2
--	COBR	COBOL I/O Subsystem
--	CPOS	DMS-B2
--	CRN	COBOL 74 RUN Unbundled
--	CRUN	CRUN Unbundled
CWGA	CWGA	COBOL I/O Subsystem
CWGB	CWGB	COBOL I/O Subsystem
CWGC	CWGC	COBOL I/O Subsystem
CWGD	CWGD	COBOL I/O Subsystem
CWGH	CWGH	COBOL I/O Subsystem
CWGI	CWGI	COBOL I/O Subsystem
--	DABF	DMS-B2 Unbundled
--	DABR	DMS-B2 Unbundled
--	DABT	DMS-B2
--	DACL	DMS-B2 Unbundled
--	DAFT	Undocumented
DATA	DATA	DATABASIC Program Language
DBAN	DBAN	DATABASIC Subsystem

6.4 Function	7.2B Function	Description
DBCR	DBCR	DATABASIC Subsystem
DBCS	DBCS	IDS Subsystem
DBDE	DBDE	DATABASIC Subsystem
--	DBGA	ADMN Unbundled
--	DBGB	ADMN Unbundled
DBLP	DBLP	DATABASIC Subsystem
DBRT	DBRT	DATABASIC Subsystem
DBVE	DBVE	DATABASIC Subsystem
DCLT	DCLT	IDS Subsystem
--	DESC	DMIV Unbundled — mods subsystem
--(WWDI)	DIAL DIRU	DMIV Unbundled
--	DMIV	DMIV Unbundled — "
--(WWLI)	DMPA OMLI	ADMN Unbundled
--	DMPB	ADMN Unbundled
(WWUP)	DMUP	MDQS Subsystem
--	DOPN	Undocumented
--	DRUN	DMS-B2
--	DRPS	Undocumented
DSTS	DSTS	DMS-B2
--	DTAB	TSS Abort Processor
--	DTCO	TSS General OPSN Overlay
--	DTGF	TSS - Mass Media Processing
--	DTLS	TSS - Mass Media Volume Swapping
--	DTUF	Undocumented
--	DUFS	DMS-B2 Unbundled
EXUT	EXUT	Undocumented
FDUM	FDUM	FDUMP, dump file of any format
FORT	FORT	FORTRAN Program Language
--	FRN	COBOL Unbundled
--	GRID	GRID Subsystem
--	GTFL	File and Record Processing
IDSQ	IDSQ	IDS Subsystem
--	IIDS	IDS Subsystem
JDAC	JDAC	DAC with User Program
JOVI	JOVI	JOVIAL Program Language
--	JRUN	Job Submission Subsystem
--	JRN	CONV Subsystem
LDSP	LDSP	IDS Subsystem
LODS	LODS	Load Debug Trace with TSS Subsystem
LODT	LODT	LODS for User Program on H* File
LODX	LODX	Load/Execute H* File
--	MAIL	Electronic Mail Unbundled Software
MAST	MAST	Master Subsystem
**	MAS2	Master Subsystem
--	MDPC	DMIV Unbundled
--	MDP2	DMIV Unbundled
--	MDP3	DMIV Unbundled

6.4 Function	7.2B Function	Description
--	MDP4	DMIV Unbundled
--	MDPG	DMIV Unbundled
--	MDRU	DMIV Unbundled
NEWU	NEWU	Sign-on New Userid/WWMCCS LOGOFF
OFLD	OFLD	IDS Data Query
OPRM	OPRM	IDS Subsystem
OREC	OREC	IDS Subsystem
PERF	PERF	MDQS Perform Subsystem
--	PLUS	DMIV Unbundled
***	PRIV	MDQS Subsystem
PSWD	PSWD	IDS Subsystem
QANL	QANL	IDS Subsystem
RECO	RECO	Current File Recovered if System Crash
--	RTFL	File and Record Processing
RUNY	RUNY	Run Command For FORTRAN
SABT	SABT	Peek Users Program after abort
--	SCAF	File and Record Processing
--	SWSA	Security Subsystem
--	SWSP	Security Subsystem
--	SORT	Time Sharing COBOL Subsystem
TCON	TCON	TCON Subsystem
--	TEX	TEX Unbundled
TRACE	TRAC	Peek/Patch User Core/H* File
TRFL	TRFL	IDS Subsystem
TSAR	TSAR	Create UST for TSS Accounting Report
TSRI	TSRI	Periodic Display of TSS Accounting Report
--	TTEX	TEX Unbundled
--	WISP	WISP Subsystem
YFOR	YFOR	FORTRAN Program Language
.YLDB	YLDB	Loader for FORTRAN Compiler
--	.DM0	DMIV Unbundled
--	.DM1	DMIV Unbundled
--	.DM2	DMIV Unbundled
--	.DM3	DMIV Unbundled
--	.DM4	DMIV Unbundled
--	.DM5	DMIV Unbundled
--	.DM6	DMIV Unbundled
--	"	DMS-B2
.YP0	.YP0	FORTRAN Compiler Overlay
.YP1	.YP1	FORTRAN Compiler Overlay
.YP2	.YP2	FORTRAN Compiler Overlay
.YP3	.YP3	FORTRAN Compiler Overlay
.YP4	.YP4	FORTRAN Compiler Overlay
.YP5	.YP5	FORTRAN Compiler Overlay
.YP6	.YP6	FORTRAN Compiler Overlay
.YLD	.YLD	Loader for FORTRAN Compiler

2.4.2 Allowed Functions. The following subsystems will be available to the restricted user:

6.4 Function	7.2B Function	Description
ABC	ABC	calculator
ACCE	ACCE	create, delete, modify files/subcatalogs
---	ADFQ	MDQS Subsystem
APRI	APRI	print ASCII file
ASCA	ASCA	convert old ASCII format to new
ASCB	ASCB	ASCII to BCD conversion
AUTO	AUTO	automatic line numbers
BCDA	BCDA	BCD to ASCII conversion
B3RU	B3RU	MDQS Subsystem
BPRI	BPRI	print file
BPUN	BPUN	punch file
BSED	BSED	line editor
BSEQ	BSEQ	basic resequence
BYE	BYE	log-off command at any level
CATA	CATA	list files in user's catalogs
(WWBC)	CMDQ	MDQS Subsystem
---	CODE	encrypt file
---	CONN	reconnect terminal
---	CONV	Convert Subsystem
---	CPY	copy file
---	DECO	de-encrypt file
DELE	DELE	delete line(s) from current file
DFAU	DFAU	MDQS Subsystem
--- (~~WWDI~~)	~~DIRU~~	~~MDQS Subsystem~~
---	DISP	Convert Subsystem print
DJST	DJST	MDQS Subsystem
--- (~~WWLI~~)	~~DMLI~~	~~MDQS Subsystem~~
---	EBLD	System level build input
EDBN	EDBN	build mode for Text Editor
EDIT	EDIT	Phase I of Text Editor
EDTX	EDTX	Phase II of Text Editor
ERAS	ERAS	erase file space/but do not release
---	FORM	form feed
GET	GET	get file
HELP	HELP	detailed explanation of system error codes
HOLD	HOLD	withhold TSS messages
JABT	JABT	abort program
JMES	JMES	status message for last job submitted
JOUT	JOUT	inspect batch output
---	JPRI	Convert Subsystem print
---	JPUN	Convert Subsystem punch
JSTS	JSTS	execution status of user's program
---	LCAS	set lower case
LEAD	LEAD	punch paper tape leader

6.4 Function	7.2B Function	Description
LENG	LENG	report length of file
LINE	LINE	set length of input line
LIST	LIST	list current file
LOGO	LOGO	log-off command at system level
---	MDP5	MDQS Subsystem
---	MDPC	MDQS Subsystem
---	MDPQ	MDQS Subsystem
(WWDM)	MDQ	MDQS Subsystem
NEW	NEW	Start new current file
---	NFOR	no form feed
NOPA	NOPA	check on noparity
OLDN	OLDN	get old or new file
PARI	PARI	check on parity
PERM	PERM	copy current file to permanent file
PRIN	PRIN	print current file
PURG	PURG	purge a file from system
PWSS	PWSS	password overstrike
REDI	REDI	MDQS redirect
RELE	RELE	release a file from system
RESA	RESA	resave a file
RESE	RESE	resequence line numbers in current file
REMO	REMO	remove file(s) from AFT
RUNO	RUNO	formats and prints a file
SAVE	SAVE	save current file and attach permissions
SCAN	SCAN	scan current file
SEND	SEND	send TSS messages
---	SEQU	non-BASIC resequence
SINI	SINI	MDQS Subsystem
****	SMCL	SMC list
STAT	STAT	user's accounting info/lists open files
STAT FILES	STAT FILES	list open files in AFT
---	STRIP	strip line numbers/blanks
*	SYST	system level
TAPE	TAPE	prepare for paper tape input
TERM	TERM	log-off command
TSEC	TSEC	classify output and files created
(WWTU)	TUTO	MDQS Subsystem
---	UCAS	set upper case
WWP2	WWP2	MDQS Subsystem
WWP3	WWP3	MDQS Subsystem
WWP4	WWP4	MDQS Subsystem
WWP5	WWP5	MDQS Subsystem
WWPC	WWPC	MDQS Subsystem
WWPG	WWPG	MDQS Subsystem
WWPQ	WWPQ	MDQS Subsystem
---	-	Text Editor

NOTE: An -- means that the subsystem did not exist under W6.4 but has functions that should be restricted in 7.2B. These functions would allow the SACLANT restricted user access to subsystems with powerful capabilities like those restricted under W6.4.

--- means that the subsystem did not exist under W6.4, but has functions that should be allowed in 7.2B.

* means that the card subsystem is not required in 7.2B, the system starts the user in the build mode. If a user wants to get back to this state, he can do so by using the SYST subsystem.

** means that MAS2 in 7.2B comprises several subsystems under W6.4. These are: MESS, MONJ, MUPD, PRIO, STUS, TALK, UPDA, and WHOS.

*** means that PRIV was allowed under W6.4, but since it is restricted by UPS there is no problem restricting it in 7.2B.

**** means that the SMCL subsystem was inhibited in W6.4 because it was a master mode subsystem to create System Master Catalogs, while in 7.2B SMCL is used to perform a similar function to CATA, which is allowed under W6.4.

( ) means that the 7.2B function is essentially identical to the W6.4 term referenced here.

SECTION 3. MDQS SUBSYSTEM

3.1 General. This section discusses the security within MDQS, relevant to preventing a restricted user from penetrating outside the MDQS environment.

The restrictions must be provided without any modifications to MDQS itself. The User Profile Subsystem (UPS) allows the Data Base Administrator (DBA) to maintain control over the use of MDQS software by the individual user and can be utilized in these security functions. UPS controls maintained for the restricted user will be reasserted by the modifications to TSS. Illegal functions within MDQS will be flagged in the program descriptors, just as illegal TSS functions are flagged. However, a security violation will occur only if UPS controls fail, or are improperly implemented. The remaining restrictions will be identified as each of the MDQS commands are discussed.

3.2 Program Descriptor. MDQS is entered by the user requesting "MDQ" from TSS. TSSH, the Time Sharing controller of user processes, searches the list of program descriptors. The program descriptor for MDQ is:

```
WDMS    PRGDES    MDQ(WWB3CL,14),,.BCMCL
```

From this program descriptor, the following information is available:

a. the program descriptor name is WDMS

b. the command list begins at the address WWB3CL and contains 14 commands

c. the subsystem uses the common command list, which is always searched prior to the subsystem command list

3.3 TSS Commands Available to MDQS. The Time Sharing common command list contains the following commands which are available to MDQS users (*indicates commands disallowed by the TSS modifications):

ABC	CONN	GET	*LODX	REMOVE
ACCESS	CONV	HELP	LOGO	RESAVE
*ADMN	*COUT	HOLD	LUCID	REW
*ALGO	*CPOS	*IDSQ	*MAIL	*ROLLBACK
*APL	CPY	*IIDS	MARK	RUNO
APRINT	*CRN	JABT	*MAST	*SABT
ASCA	*CRUN	*JDAC	MDQ	SAVE
ASCBCD	*DABT	JOUT	NEW	SCAN
AUTO	*DATA	*JOVI	*NEWU	SEND
*BASI	DECODE	JPUNCH	NFOR	SEQU
BCDASC	DELE	JPRINT	NOPA	SMCL
BPRINT	DISPLAY	*JRN	OLD	STAT
BPUNCH	*DMIV	JSTS	PARI	STRIP
*BRN	DONE	LCAS	PERM	SYSTEM
BSEQU	*DRUN	LEAD	PRINT	TAPE
BSP	*DSTS	LENG	PTOF	*TEX
BYE	EDIT	LEVEL	PTON	*TSAR
*CARD	ERASE	LIB	PURG	UCAS
CATALOG	*FDUMP	LINE	READ	WRIT
*CIDS	FORM	LIST	RECLASSIFY	*YFOR
CLASSIFY	*FORT	*LODS	*RECOVER	-
*CMOD	*FRN	*LODT	RELEASE	*"
CODE				

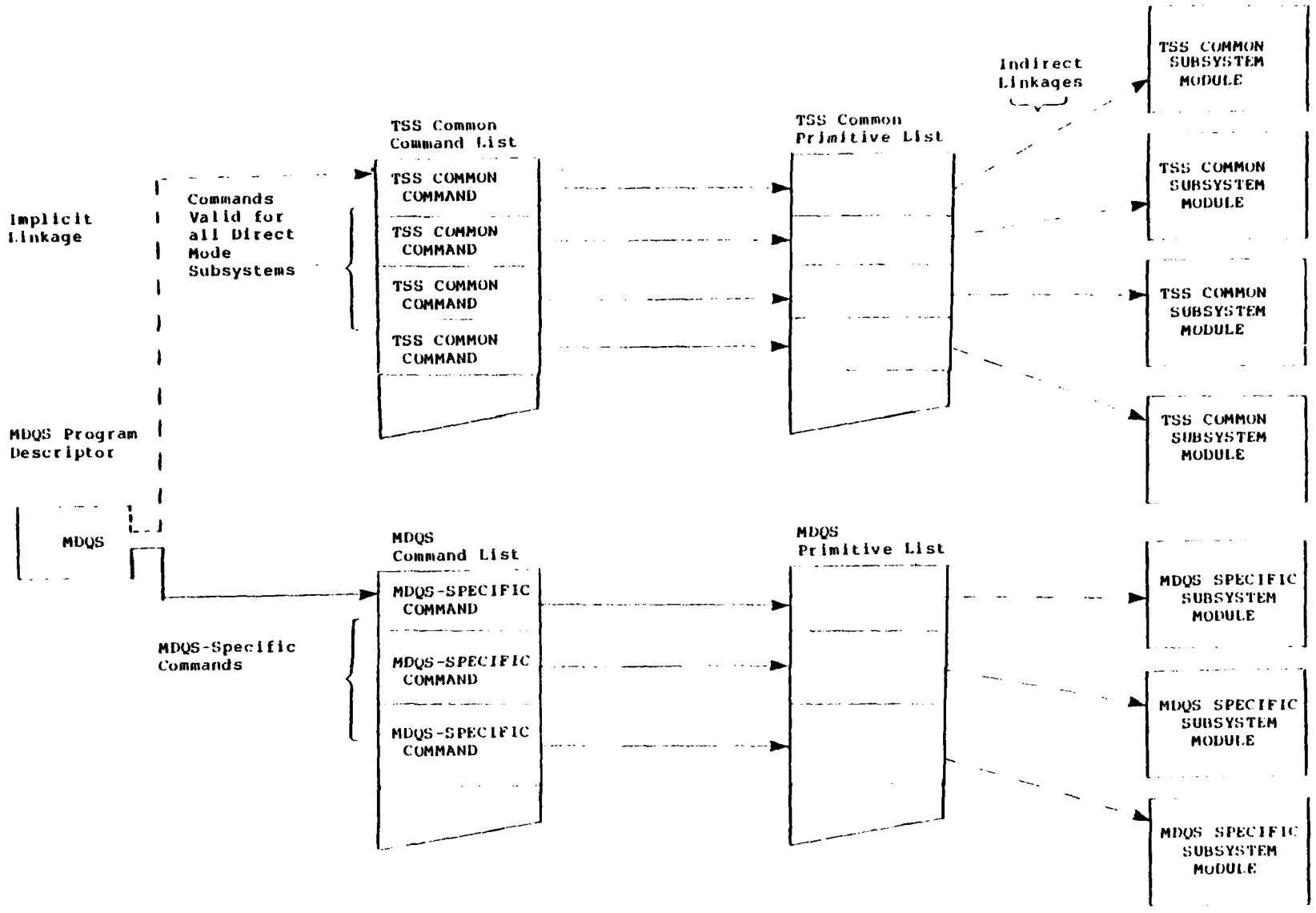


Figure 3-01. MDQS Direct Mode Subsystem Structure

3.4 MDQS Commands. The MDQS commands available are:

ADFQ	DMUP
CHECK	PERF
CMDQ	PRIV
DFAU	REDI
DIRU	RUN
DJST	SINI
DMLI	TUTO

The discussion of each of these commands will be as follows:

a. Functional Description. A description of the command's function.

b. Modules Involved. The modules that process the command and the exits outside the MDQS environment.

c. Security Recommendations. The steps to be taken to secure the restricted user.

3.4.1 ADFQ.

3.4.1.1 Functional Description. The ADFQ command invokes a question/answer sequence to allow the MDQS user to examine the user-visible contents of the object Application Definition File (ADF).

3.4.1.2 Modules Involved. ADFQ is processed by TXGD with the only calls outside of MDQS being to .GBCD (File and Record Control BCD conversion) and the Time Sharing subsystem REDI.

3.4.1.3 Security Recommendations. None.

3.4.2 CHECK.

3.4.2.1 Functional Description. CHECK allows an MDQS user to have a specified procedure checked for syntax analysis before it executes the procedure.

3.4.2.2 Modules Involved. CHECK is processed as the RUN command; reference 3.4.12.2.

3.4.2.3 Security Recommendations. None.

3.4.3 CMDQ.

3.4.3.1 Functional Description. CMDQ invokes a question/answer sequence by which a MDQS procedure is generated and passed to the MDQS syntax analyzer for processing.

3.4.3.2 Modules Involved. CMDQ is processed by TXGL with calls to the MDQS subsystems ADFQ and B3RU and to the Time Sharing subsystems LIST, SAVE, and RESAVE.

3.4.3.3 Security Recommendations. None.

3.4.4 DFAU.

3.4.4.1 Functional Description. DFAU allows the MDQS user to display at the terminal the procedure batch fault messages accumulated on the Fault Message File when the RUNF command has been used.

3.4.4.2 Modules Involved. DFAU is processed by DEFAULT from which there are no exits.

3.4.4.3 Security Recommendations. None.

3.4.5 DIRU.

3.4.5.1 Functional Description. DIRU allows the MDQS user to build and maintain MDQS directory ~~source~~ BEST files and optionally to allocate space and to catalog the control and/or data base file.

3.4.5.2 Modules Involved. DIRU is processed by TXGA which has no exits outside of MDQS.

3.4.5.3 Security Recommendations. ~~None~~. Allows user to see database name.

3.4.6 DJST.

3.4.6.1 Functional Description. DJST allows the MDQS user to monitor the execution status of batch jobs.

3.4.6.2 Modules Involved. DJST is processed by TXGE which calls the Time Sharing subsystems JABT and JSTS.

3.4.6.3 Security Recommendations. None.

3.4.7 DMLI.

3.4.7.1 Functional Description. DMLI invokes a question/answer sequence to allow the DBA to modify both user and system subroutine libraries.

3.4.7.2 Modules Involved. DMLI is processed by TXGO with calls to the Time Sharing subsystems REMO and ACCE.

3.4.7.3 Security Recommendations. None.

3.4.8 DMUP.

3.4.8.1 Functional Description. DMUP allows the DBA to access and manipulate the UPS master file, which provides controls over the individual user's use of MDQS.

3.4.8.2 Modules Involved. DMUP is processed by TXGI with no exits outside of MDQS.

3.4.8.3 Security Recommendations. The UPS master file is protected only by FMS. The file has general read permissions with the USERID DATAMGT having read/write permissions. Immediately upon entering TXGI, an attempt is made to access the UPS file with read/write permissions. If a USERID other than DATAMGT attempts to use the DMUP command, FMS issues the following error message:

<50> NO PERMISSION

Considering the controls which are maintained by the UPS master file, the use of DMUP will be restricted by the Time Sharing alters.

3.4.9 PERF.

3.4.9.1 Functional Description. PERF allows the MDQS user to interface with batch utility programs. The different functions allow the user to build required job streams, and then to load and execute the jobs.

3.4.9.2 Modules Involved. PERF is processed by TXBG which calls the Time Sharing subsystems CDIN, LOGO, SAVE, and LIST. In addition to these direct subsystem calls, any Time Sharing subsystems will be called when the user enters the appropriate command.

3.4.9.3 Security Recommendations. Access to PERF should be denied to the restricted user. The denial can be performed by UPS, and will be implemented by the Time Sharing modifications.

3.4.10 PRIV.

3.4.10.1 Functional Description. PRIV allows the DBA to build and modify privacy files, which provide protection from MDQS procedures accessing specified items or records.

3.4.10.2 Modules Involved. PRIV is processed by TXGB with calls to the Time Sharing subsystem LOGO.

3.4.10.3 Security Recommendations. Access to PRIV should be denied to the restricted user. The denial can be performed by UPS, and is also restricted by the Time Sharing alters.

3.4.11 REDI.

3.4.11.1 Functional Description. REDI allows the MDQS user to send an ASCII file to either an online printer or a remote printer.

3.4.11.2 Modules Involved. REDI is processed by TXBS and TXBT. No calls are made outside of MDQS.

3.4.11.3 Security Recommendations. None.

3.4.12 RUN.

3.4.12.1 Functional Description. The RUN command allows a MDQS user to have a specified procedure executed. If the specified procedure is in source format, it will be checked for syntax analysis prior to execution. In addition to the RUN command, there are four variations of the RUN command:

a. RUNF. Procedure is executed and any fault messages are written to the Fault Message File to be retrieved by the DFAU command.

b. RUNS. Procedure is executed and user is continuously informed of its status.

c. RUNJ. Similar to RUNS command, except the Time Sharing subsystem JOUT is invoked upon execution completion.

d. RUNR. DAC procedure is restarted following a system restart.

3.4.12.2 Modules Involved. Processing of the RUN commands (and CHECK) is accomplished in five phases. TXEB processes the initial command scan and calls in the remaining phases as overlays. PHASE2 performs the procedure syntax analysis, PHASE3 interfaces with the Application Definition File (ADF). PHASE4 builds the Procedure Information File (PIF). PHASE5 processes the procedure options and spawns the batch job. During the processing, the following Time Sharing subsystems are called: JOUT, DJST, and JDAC (RUNR only).

3.4.12.3 Security Recommendations. Because RUNR utilizes direct access, TSS TALK permission is required; because TALK permission is by definition to be denied to the restricted user, the use of RUNR is consequently denied. There are no security problems with the remaining RUN commands.

3.4.13 SINI.

3.4.13.1 Functional Description. SINI allows the DBA to initialize and maintain the MDQS Status File (DSTATF).

3.4.13.2 Modules Involved. SINI is processed by TXGF which has no exits.

3.4.13.3 Security Recommendations. Although SINI is by definition a DBA command, it presents no security problems if it should be accessed by others; therefore no additional controls are required.

3.4.14 TUTO.

3.4.14.1 Functional Description. TUTO calls in the tutorial subsystem which provides explanations of selected portions of MDQS.

3.4.14.2 Modules Involved. TUTO is processed by TXGC which calls only File and Record Control routines for file processing.

3.4.14.3 Security Recommendations. None.

3.5 MDQS Procedure Language.

3.5.1 User Subroutine Libraries. The restricted user is to have full MDQS capabilities. A foreseeable security problem with the MDQS procedure language lies with the use of libraries. Both system and user subroutine libraries can be accessed from MDQS procedures by the use of

LIBRARY

TLU

USE_____FROM_____

statements. The use of carefully screened libraries presents no problems; but if the building of libraries from either Time Sharing or batch jobs is not carefully controlled, the sophisticated MDQS user can develop subroutines or functions by which he can travel beyond his defined limits within the H6000. Thus, in addition to preventing the restricted user from using the DMLI Time Sharing command and from running batch jobs via CARDIN, the restricted user's batch jobs should be carefully screened.

3.5.2 Transaction Data Bases. In some Time Sharing subsystems, the use of transaction data bases can present the opportunity for a sophisticated user to exit from the normal updating process. Within MDQS this is not a problem because the Data Base Administrator has control over the transaction data bases.

The following lists the procedure statements which use transaction data bases and the controls available to the DBA:

Procedure Statement	Data Base Must be Defined in ADF	UPS Control
CREATE	yes	yes
KEEP	no	yes
RETRIEVE	yes	no
UPDATE	yes	no

In addition to these procedure statements, the READ_____ INTO_____ statement utilizes a transaction data base but operates with a read from the file into the data base. Consequently, this statement presents no security problems either.

	ADFQ	CHECK	CMDQ	DFAU	DIRU	DJST	DMLI	DMUP	PERF	PRIV	REDI	RUN	SINI	TUTO
MDQS User Command	*	*	*	*	*	*			*		*	*		*
MDQS Data Base Administrator Command							*	*		*			*	
Restricted by TSS Alters								*	*	*				
Controlled By UPS									*	*		***		
Additional Controls Required								*				**		*

** RUNR
*** RUNF, RUNJ, RUNS

FIGURE 3-02. MDQS Command Summary

SECTION 4. CMDLIB

4.1 General. The following paragraphs describe the characteristics of a user-defined subsystem on the CMDLIB which are relevant to maintaining the security of the MDQS environment. Subversion can occur by using a CMDLIB subsystem through a wide variety of technical means. Hence, a subsystem can be pronounced "pure" only if it has been reviewed line-by-line. However, a few basic guidelines can be presented.

4.2 User Access. There must be a clear separation of subsystem duties from user access. For example, although a subsystem may need to provide a job execution capability, it does not mean that the user must have access to the RUN command within TSS. However, the farther the subsystem travels from the controls within TSS, the less secure the entire system is.

4.3 Data Input. If a subsystem is to allow the creation of a file that is to be executed, then the subsystem must also have a syntax review which at least checks for the attempt to input a job stream. For example, if MDQS did not check for MDQS syntax then the user could simply:

a. Build a valid query

b. Place an end of data on that file

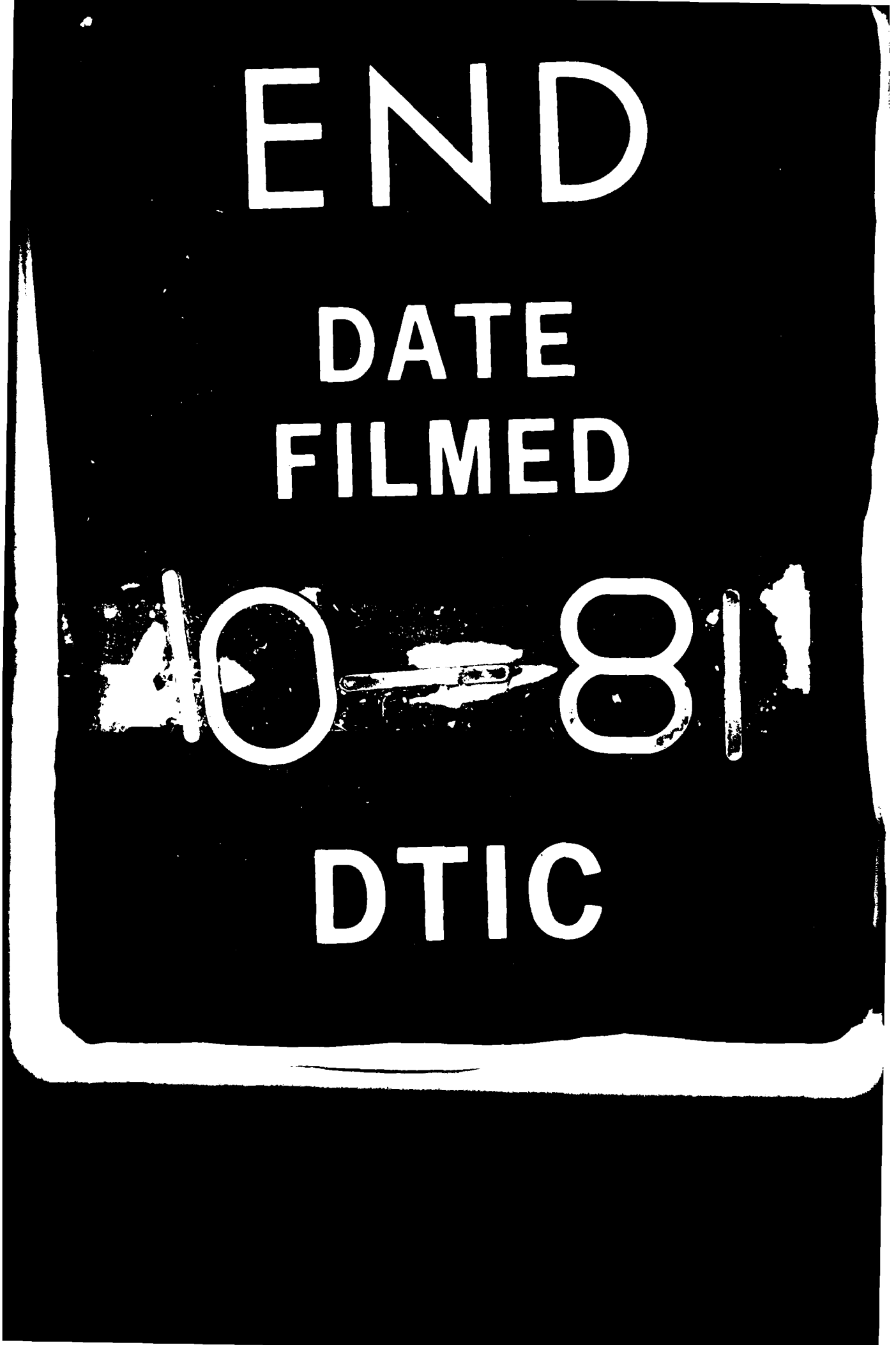
c. Place a job stream on the file which would act as an additional activity on the MDQS execution

Even though the TSS alters would prohibit a user's attempt to RUN, an attempt could still be made to use the subsystem's execution. A syntax review would effectively negate that possibility. In general, the restricted user must never be allowed to input a job stream.

4.4 Job Execution. A restricted user will never have access to CDIN, the RUN command within CARDIN and EDIT, or RUNY. A CMDLIB subsystem will not be able to do a DRL CALLSS to any disallowed subsystems; the modification to TSS should catch the attempt. Although this test was not documented, the logic of the alters should encompass this as it is now. Job execution for a CMDLIB subsystem must, therefore, be done in a MDQS-like manner with a DRL SNUMB and a DRL SPAWN.

The TCON manner of job execution must be thoroughly disallowed. TCON has CDIN, as well as TRACE, duplicated in its own coding, and is definitely beyond the control of the TSS modifications.

Any disallowed functions within TSS can be accomplished by the subsystem via DRL's. In this manner, job execution will occur from subsystem request, not the restricted user.


END
DATE
FILMED
40-81
DTIC